महिला व बालक यांच्या संदर्भातील सायबर सुरक्षिततेबाबतच्या इंटरनेट वापरताना घ्यावयाच्या काळजीबाबतच्या मार्गदर्शक सुचना.

महाराष्ट्र शासन

गृह विभाग

शासन परिपत्रक क्रमांक: बैठक २०२३/प्र.क्र.१४३/विशा-३(अ)

मंत्रालय, मुंबई-४०००३२

दिनांक: ०५. ०१.२०२४

संदर्भ: विशेष पोलीस महानिरीक्षक ,महाराष्ट्र सायबर, मुंबई यांचे पत्र क्र. १९४५/विपोमनि/सायबर व मअप्र /२०२३ यांचे दि.२१.०७.२०२३ रोजीचे पत्र.

परिपत्रक

सायबर गुन्हेगारी ही जगातील सर्वात मोठी संघटीत गुन्हेगारी म्हणून उदयास आली असुन राज्यात सायबर फसवणूकीद्वारे गुन्हे करण्याचे प्रमाण वाढले आहे. सायबर फसवणूकीला बळी पडणा-या नागरिकांना विशेषत: महिला, बालके यांना केंद्रबिंदू ठेवून महिला व बालक यांच्या संदर्भातील सायबर सुरक्षिततेबाबतच्या इंटरनेट वापरताना घ्यावयाच्या काळजीबाबतच्या मार्गदर्शक सुचना निर्गमित करण्याबाबत मा. उप सभापती महाराष्ट्र विधानपरिषद यांनी १९.०७.२०२३ रोजी विधानभवन, मुंबई येथे आयोजित केलेल्या बैठकीत सूचित केले होते. त्यानुसार उपरोक्त संदर्भाधिन पत्रान्वये विपोमनि सायबर यांनी शासनास सदर सुचनांचे प्रारुप मान्यतेस्तव सादर केले आहे. सबब सदर मार्गदर्शक सुचना निर्गमित करण्याची बाब शासनाच्या विचाराधीन होती.

२. सबब, सर्व महिला व बालकांनी सायबर गुन्ह्यांमधे फसवले जाऊ नये यासाठी इंटरनेटचा वापर करतांना दक्षता घेणे आवश्यक असुन सायबर सुरक्षतेबाबत इंटरनेटचा वापर करतांना खालील गोष्टींची काळजी घेण्यात यावी.

➤ Use Strong and Unique Passwords : सशक्त पासवर्ड तयार करतांना upper and lower case letters, numbers, and symbols चा वापर करावा. तसेच सहजतेने पासवर्डचा अंदाज घेवु शकता असे पासवर्ड ठेवण्यात येऊ नये. उदा जन्म तारीख, स्वतःचे नाव, मोबाईल नंबर इत्यादी तसेच प्रत्येक नवीन अकांउटकरीता वेगळा पासवर्ड ठेवण्यात यावा. वेळोवेळी सर्व पासवर्ड हे बदलावेत व कोणतेही अकांउट लॉगीन करतांना पासवर्ड हे ब्राउझर मध्ये SAVE करण्यात येऊ नयेत.

➤सर्व सोशल मिडीया अकांउट व ऑनलाइन सर्व अकांउटकरीता Two-Factor Authentication (२FA) ON ठेवणे गरजेचे आहे. ऑनलाइन लॉगीन करतांना तुमच्या फोनवर पाठवलेल्या कोडने हे दुस-या स्वरूपाच्या पडताळणी करून सुरक्षितेकरीता अतिरिक्त स्तर जोडते. सबब, Two-Factor Authentication (२FA) ON ठेवण्याबाबत दक्षता घ्यावी.

➤**सॉफ्टवेअर अपडेटेड ठेवा** : तुमचे operating system, applications, and antivirus software हे नियमितपणे अपडेट करा. सॉफ्टवेअर अपडेटमध्ये अनेकदा vulnerabilities संदर्भातील security patches देखील असतात त्यामुळे होणारे संभाव्य धोके टाळता येतील.

➤ **Beware of Phishing Attempts :** अनपेक्षीत प्राप्त होणारे मेल, मॅसेज किंवा वैयक्तिक माहिती विचारणारे कॉल, संशयास्पद लिंक्स असलेले मेसेज पासुन सावध रहा. खात्री केल्याशिवाय कोणत्याही लिंक्स वर क्लिक करू नका. तसेच कोणतेही attachments download करू नका जेणेकरून नकळत Background ला कोणतेही Software run होणार नाही.

➤**Use Secure Wi-Fi Networks :** ऑनलाइन वैयक्तिक व संवेदनशील माहितीचा वापर करतांना सुरक्षित Wi-Fi Networks चा वापर करावा. तसेच संवेदनशील माहिती तसेच ऑनलाईन आर्थिक व्यवहार करतांना सार्वजनिक Wi-Fi Networks चा वापर करणे टाळावे.

➤ **Back Up Your Data Regularly :** महत्वाच्या फाइल्स व डेटाचा नियमितपणे external storage device or a secure cloud service मध्ये बॅकअप घेण्यात यावा. जर आपल्या सिस्टीममध्ये ransomware attack or hardware failure झाल्यास डेटा बॅकअप घेतल्यामुळे डेटा गमावणे टाळता येईल.

➤ **Use a Firewall:** तुमच्या संगणक व नेटवर्कचा फायरवॉल हा ON असल्याची खात्री करा. जेणेकरून तुमच्या सिस्टीममध्ये अनाधिकृत प्रवेश रोखण्यास मदत होईल.

➤**Practice Safe Social Media Habits :** सोशल मिडीयावर वैयक्तिक माहिती शेअर करू नका. तसेच सोशल मिडीयाच्या सर्व अकांउटला Privacy सेटींग ठेवा. उदा प्रोफाइल लॉक करणे, आपली वैयक्तिक माहिती फक्त आपल्या मित्र,मैत्रीण, परिचयाचे लोकांनाच दिसेल याबाबत आवश्यक काळजी घ्यावी.

➤**Log off:** प्रत्येक वेळी कोणतेही ऑनलाईन ॲप तसेच सोशल मिडीया अकांउट लॉगीन केल्यांनतर त्याचा वापर झाल्यानंतर ते लॉग आउट करून ते लॉग आउट झाले असल्याची खात्री करण्यात यावी.

➤**Don't Share information more than requirement:** ऑनलाईन अथवा सोशल मिडीयावर संपर्कात येणाऱ्या कोणत्याही अनोळखी व्यक्तीला आपली वैयक्तिक माहिती उदा पत्ता, फोन नंबर, स्वतःचे वैयक्तिक अथवा खाजगी फोटो शेअर करु नयेत. त्याचा दुरुपयोग आपणास सेक्टॉर्शन अथवा ब्लॅकमेल करण्यासाठी होऊ शकतो सबब याबाबत दक्षता घेण्यात यावी.

➤**Don't Meet your online friend alone:** ऑनलाईन अथवा सोशल मिडीयावर संपर्कात येणाऱ्या कोणत्याही खात्रीशीर न वाटणाऱ्या अनोळखी व्यक्तीला प्रत्यक्षात एकटे भेटणे टाळावे. अशा व्यक्तीस शक्य असल्यास सार्वजनिक ठिकाणी भेटावे जेणेकरुन भविष्यातील संभाव्य फसवणूकीचे धोके टाळणे शक्य होईल.

➤**Keep your Webcam off :** इंटरनेटवर उपलब्ध असणारे काही ॲप्लिकेशन्स हे तुमचा वेबकॅम तुमच्या माहिती शिवाय ॲक्सेस करु शकतात म्हणुनच शक्य असल्यास वेबकॅम बंद ठेवावा अथवा त्याचे वर कव्हर लावण्याबाबत दक्षता घ्यावी.

➤Avoid downloading free stuff : इंटरनेटवर मोफत उपलब्ध असणारे गेम्स, ॲप्स अथवा सिनेमा अनोळखी अथवा Untrusted sites वरुन डाऊनलोड करणे टाळावे. त्यामध्ये स्पायवेअर अथवा व्हायरस, रॅन्समवेअर असण्याची शक्यता नाकारता येत नाही.

➤Use parental control: आपले घरातील स्मार्ट डिव्हाईसेस उदा. मोबाईल फोन, कॉम्प्युटर जर अल्पवयीन मुले वापरत असतील तर parental control सेटींग्स चा वापर करण्याबाबत खातरजमा करावी.

सदर शासन परिपत्रक महाराष्ट्र शासनाच्या www.maharashtra.gov.in या संकेतस्थळावर उपलब्ध करण्यात आला असून त्याचा संकेताक २०२४०१०८१७५६०९८८२९ असा आहे. हा आदेश डिजीटल स्वाक्षरीने साक्षांकित करुन काढण्यात येत आहे.

महाराष्ट्राचे राज्यपाल यांच्या आदेशानुसार व नावाने.

RAHUL VIJAY KULKARNI

Digitally signed by RAHUL VIJAY KULKARNI
DN: c=IN, o=GOVERNMENT OF MAHARASHTRA, ou=HOME DEPARTMENT, 2.5.4.20=019d1a40755cacf50cb371c432c67afaec7da5aad928d966ad4270c6a4f1ac39, postalCode=400032, st=Maharashtra, serialNumber=31493D4A6291F531ED8FD00972CCBFA0376623C7F6C38C3B848BFBE06685A219, cn=RAHUL VIJAY KULKARNI
Date: 2024.01.08 17:55:27 +05'30'

(राहुल कुलकर्णी)
सह सचिव,महाराष्ट्र शासन

प्रत,

१. मा. मुख्यमंत्री यांचे प्रधान सचिव, मंत्रालय, मुंबई.
२. मा. उपमुख्यमंत्री (गृह)यांचे सचिव, मंत्रालय, मुंबई.
३. मा. उपमुख्यमंत्री (वित्त व नियोजन) यांचे सचिव, मंत्रालय, मुंबई.
४. अपर मुख्य सचिव / प्रधान सचिव/सचिव, यांचे स्वीय सहायक, सर्व मत्रालयीन विभाग, मंत्रालय, मुंबई.
५. प्रधान सचिव (विशेष), याचे स्वीय सहायक, गृह विभाग, मंत्रालय, मुंबई
६. पोलीस महासंचालक, महाराष्ट्र राज्य, मुंबई.
७. अपर पोलीस महासंचालक (नि.व.स) महाराष्ट्र राज्य, मुंबई.
८. मा. महालेखापाल (लेखा व अनुज्ञेयता / लेखा परीक्षा), महाराष्ट्र, मुंबई / नागपूर.
९. विशेष पोलीस महानिरीक्षक, महाराष्ट्र सायबर, मुंबई.
१०. निवड नस्ती (विशा-३)